Sanlam Employee Benefits Information Security Statement

The need for Information Security has dramatically increased in the digital age. With updated legislation, regulatory interventions and demand from our stakeholders, Sanlam acknowledges the need to ensure that we remain compliant as well as ensure that we secure all the information we manage in line with worldwide best practice principles. Securing the information we manage is a crucial part of what we do and how we do it.

Sanlam has a formal Information Security Strategy, inclusive of Cyber Crime, to which Sanlam Employee Benefits subscribes. The strategy is driven and governed by the Sanlam Group Office and the execution of the controls and preventative processes are co-ordinated and executed by Sanlam's Group Technology and Information division. Governance is via a number of governance forums (representing all the businesses in the Sanlam Group) that reports quarterly to the Group Office and the Sanlam Board. Our strong focus on governance ensures that the business culture is aligned with the efforts put in place to secure the information we manage.

The following are focus areas for Sanlam:

1. Protection of Personal Information

Although part of the information security structures, a dedicated privacy protection project was launched to ensure that the compliance requirements and privacy policies required to align with the POPI Act are aligned and implemented throughout the Group. The privacy protection project deals with protection of personal information and data privacy when information is processed by Sanlam, and aims to embed a group wide framework for the responsible handling of personal information which is applicable to privacy related laws, regulations and internal policies. The protection of personal information has been incorporated throughout the information security management process.

2. Information Risk Management Regime:

An Information Management Framework was developed to ensure the appropriate structures are in place to support the Sanlam Group's commitment to information security. Formal policies and processes are in place to monitor, identify and mitigate information risk. A strong focus is placed on both logical and physical security to ensure that client information is secure and treated as confidential. A clean-desk policy is promoted and client information will only be shared with authorised third parties.

3. Business Continuity (BC) and Disaster Recovery (DR):

Formal BC and DR plans in place to ensure that interruption to operations is limited during an unplanned disaster. These plans include (but are not limited to):

- High availability configuration of systems with continuous syncing of data between two separate data centres.
- Dedicated off-site facilities for hosting staff during such an event and the capability for staff to access systems to work from home.

DR tests are typically done twice a year. If not done as part of the DR tests, BC plans are tested as scheduled by business management.

Sanlam Employee Benefits

2 Strand Road, Bellville 7530 | PO Box 1, Sanlamhof 7532, South Africa

T +27 (0) 21 947 9111

4. Capacity Management

A formal Capacity Management Policy and Process has been developed and implemented. Capacity is monitored 24/7 and all incidents/issues are reported to the IT Operations Managers who ensure the incidents are addressed before processing is impacted.

5. User Education and Awareness

Group Office and business unit risk & compliance managers implement regular actions to increase user education and awareness. These include information campaigns (both formal and informal) with some of them requiring staff to formally sign-off and/or complete a “test”.

6. Incident Management

Incident management (information or cyber related) is done via a formal process with a Cyber Security Incident Response Team (CSIRT). All incidents are reported to Sanlam Group Office and Sanlam Board and managed in line with the appropriate policy.

7. Managing User Privileges

Logical access is key to our business and processes. Formal tools and security teams are in place for managing this on all levels, including: network, server, desktop and external (via the Firewalls). This is audited on a regular basis.

8. Removable Media Controls

A number of projects are currently underway to ensure all the requirements regarding this is implemented as prescribed by legislation. These include items like port blocking, encryption of data on hard drives of PC’s/Laptops, encryption of e-mails, etc. Many of these projects have already been completed and implemented.

9. Monitoring

Sanlam Information Security department appointed dedicated teams to monitor activities on our network and devices. These include the monitoring and response to potential cyber threats and internal activities that may be deemed to be suspicious. The CSIRT, respond to potential incidents. Sanlam participates in national and international cyber-crime prevention forums where potential harmful activities are shared which allow Sanlam to configure stronger monitoring and controls.

10. Secure Configuration

Sanlam has adapted a strategy of “secure development” and has developed a formal course that developers are put through to vest the behaviour. Industry standards are followed when hardening operating systems and data base platforms to ensure best practice solutions.

11. Malware Protection

Sanlam has a group wide strategy regarding the software utilised to perform malware protection. All business units, including new entrants, need to comply before allowed on the network. This is further being enhanced by deploying advanced threat detection and preventative mechanisms to provide better protection against zero-day attacks and ransomware.

12. Network security

Although network security is covered in many of the above items, it is worth mentioning that it is a high priority focus that is being monitored closely and enforced diligently.

13. Home and Mobile Working

Sanlam supports mobile and home work, but only via approved devices and secure virtual private networks. Policies are in place to ensure individuals who make use of this are informed of the risks as well as our policies relating to mobile and home work.

More on Sanlam and Cyber-resilience

The threat that cyber risk poses to our client data, our technology and our brand is top priority for the Sanlam Board and Exco.

We view it as the type of risk that threatens the very continuity of our Business and that it is quite unique in its nature, is forever adapting and changing and has the ability to move beyond the physical barriers used to contain traditional catastrophic risks.

Sanlam shares the view of the World Economic Forum, the various regulators and industry bodies that the defence strategy against the cyber threat must necessarily include collaboration with other role players. Sanlam is therefore playing an active role in the financial services' Computer Security Incident Response Team (CSIRT) and in sharing threat and response intelligence with the CSIRT's of other industries. Sanlam is also actively engaging with the Financial Services Information Sharing and Analysis Centre's (FS-ISAC) Europe and Africa operations. Sanlam furthermore supports the notion that one needs to develop resilience to deal with cyber incidents. As part of business continuity management process, senior leadership and technical management participate in cyber crisis simulations to prepare them to deal with a cyber-crisis.

In response to the risk Sanlam adopted a cyber-resilience strategy with 5 focus areas namely Intelligence (or early warning), protection, monitoring, detection and response (which includes cyber incident and crisis management).

Sanlam utilises international best practice risk assessment methodologies to identify and focus our efforts on our mission critical information resources. Sanlam also recognise that all entry and exit avenues in the network, on our systems and in our security processes need to be secured and are therefore continuously focussing on this.

Sanlam's monitoring and detection capability is further supported by technology that deals with masses of data. This enables us to sift through data, looking for anomalies or trends that could potentially be harmful. Our staff are formally educated and certified in these techniques and are kept up to date through simulations by our cyber consultancies and Sanlam endeavours to keep improving their capability and maturity.

Sanlam continuously monitors emerging threats and adapts our controls in response to these, focusing specifically on any new advanced threat mitigation techniques. Sanlam's information security management system has been in existence since 2001. We have been ISF members since 2000 and frequently take part in their security benchmark.